Written Statement of the Honorable Charles R. Christopherson, Jr.
Chief Financial Officer
U.S. Department of Agriculture

Before the
Agriculture Committee
The U.S. House of Representatives
May 2, 2007

Mr. Chairman, Ranking Member Goodlatte, and members of the Committee, thank you for your invitation to appear before you today to update the Committee on current events related to information technology at the United States Department of Agriculture (USDA).

I am Charles Christopherson, Chief Financial Officer at USDA. My role with respect to information technology is to ensure that the financial systems throughout the Department work together and protect the security of financial information. I am joined today by Dave Combs, the Department's Chief Information Officer (CIO) and Senior Agency Official for Privacy; and Boyd Rutherford, our Assistant Secretary for Administration.

We are here today primarily because of the recent discovery that approximately 38,700 Social Security Numbers (SSNs) had been inadvertently made public through a government-wide system known as the Federal Assistance Awards Data System (FAADS). This information was also reposted by other commercial or non-profit websites. At the outset, let me state that we take full responsibility for this incident and offer no excuses. We regret the exposure of this sensitive information (by sensitive information we mean personally identifiable information about individuals) and the concern it has caused the citizens we serve.

In my testimony today, I would like to achieve four principal goals. First, to provide the context for this incident, I would like to provide some basic information about USDA's information technology portfolio and our ongoing efforts to protect sensitive information. Second, I will brief the Committee on the facts of the incident. Third, I will describe for the Committee exactly how we are taking responsibility and implementing corrective action, in light of this incident. Finally, I will take a few moments to update the committee on our ongoing efforts to further bolster our overall information security.

Background on Protection of Sensitive Information

USDA is comprised of Departmental headquarters, 17 component agencies, and 12 staff offices. We have approximately 100,000 employees located in some 7,200 offices throughout the world. Each of the 17 agencies has a Chief Information Officer who oversees IT systems and processes; many of which have evolved over many years. Many of our systems date back to the early days of computing, before the internet, and before the identity theft challenges of the modern information age.   As a result, more than 250 IT systems were developed over the course of several decades. Personal information, such as SSNs, were used as customer identifiers, and thus were key to accessing records in many of these older, legacy systems.

In this new era, where individuals must guard themselves against the risks of identity theft, these old ways of doing business are no longer acceptable. Unfortunately, our complex tapestry of systems cannot be unwound by pulling on a single thread. Rather, it requires a sustained and coordinated effort that simply takes more time than we would like, as well as substantial resources.

Let me assure you, that we did not just wake up to this challenge last week. Addressing these issues has been an ongoing effort. For the past several years, we have been working on implementation of the Federal Information Security Management Act (FISMA). FISMA is a law which provides a framework to protect all Federal information – including sensitive and personally identifiable information. In USDA's most recent quarterly Federal Information Security Management Act (FISMA) report, a total of 56 systems were identified as containing sensitive information. These information systems are secured based on the type of information which they contain. When a system is found to be maintaining or transmitting personally identifiable information – we protect it using a set of security controls developed specifically for high and/or moderate impact information systems. In Fiscal Year (FY) 2006, we took several important steps. Let me provide a few examples. On June 22, 2006, OCIO issued a memo entitled "Management of Privacy Act Data" to all USDA agencies requiring a complete inventory of all systems that store or process data protected under the Privacy Act, and directing a review of all operations to determine compliance with Department policy. While this memo did not explicitly address the use of embedded SSNs, it did set into motion a process to identify and thoroughly scrub all improper and unnecessary uses of personally identifying information. This was followed by a July 13, 2006, directive to implement the recommendations of OMB Memorandum 06-16, including actions to encrypt all mobile computers and to install two-factor authentication for remote access to

USDA systems. In addition, all USDA employees and contractors were required to complete a "USDA Privacy Basics" course between July 18, 2006, and September 15, 2006.

In response to a recommendation from the President's Taskforce on Identity Theft, Mr. Rutherford and I sent a memorandum to the users of the financial and human capital systems explaining the breadth of their responsibilities concerning information protected under the Privacy Act. The memorandum states: "To be clear, safeguarding people's sensitive information is not an option, it is a responsibility engrained into every financial and human resources position." Since August 2006, USDA organizations including the Office of the Chief Financial Officer have held additional privacy information training sessions and worked to remove social security information from reports.

On October 5, 2006, we amended Standard Operating Procedure (SOP) to assist the United States Department of Agriculture (USDA), Computer Incident Response Team (CIRT) in processing reports of computer security events. This SOP is designed to assist the security analyst in determining which events should be elevated to incidents, and which events should be escalated to United States Computer Emergency Readiness Team. The document also outlines procedures for dealing with different types of events and incidents, the requirements for escalating incidents to senior officials, and for facilitating CIRT interactions with other organizations, both internal and external to the Department.

On April 6, 2007, the Department added to the Senior Executive Service (SES) Performance Standard the requirement that "ensures 100 percent of the workforce (Federal and contractors) have successfully completed the Computer Security Awareness and Privacy Refresher training. All new employees/contractors with access to Information Technology (IT) systems receive a security briefing prior to access being granted." Each of our SES leaders provides an important management role in protecting privacy information.

Prior to the recent incident, the three of us (the Chief Financial Officer, the Chief Information Officer, and the Assistant Secretary for Administration) had already commenced working on eliminating unnecessary usage of SSNs as an identifier at USDA. To date, this project has eliminated unnecessary usage for approximately 29,500 individuals. We also initiated a requirement that each employee and contractor with access to information technology systems or personal privacy information take Privacy Act training. The continuing training program is used to reinforce the fact that every person is responsible for protecting sensitive information.

On October 26, 2006, under the guidance of the Office of Management and Budget (OMB), USDA established its Identity Core Response Group led by the Chief Information Officer, and consisting of the Chief of Staff, General Counsel, Assistant Secretary for Administration, Assistant Secretary for Congressional Relations, the Director of the Office of Communications, the Inspector General, and other members as needed on an incident basis. The idea motivating the creation of this group was that, notwithstanding best efforts to mitigate the risks of disclosure of sensitive information, we needed to be prepared for any unforeseen incidents that might arise. Having this structure in place was essential in allowing us to respond as swiftly as we did to the incident that brings us here today.

The Recent Incident:

On Friday, April 13, 2007, USDA learned that a grantee was surfing the internet and noticed that her company's identifying information was posted on the website fedspending.org (a data base created and maintained by the OMB Watch organization which draws grant and contract information from two federal data bases: the Federal Assistance Award Data System and the Federal Procurement Data System). The number was not identified as a SSN or Employer Identification Number (EIN), but was instead embedded as nine numbers within a larger data field in a database known as the Federal Assistance Award Data System (FAADS).

FAADS was established pursuant to the Consolidated Federal Funds Report Act of 1982. That Act and successor laws require Federal agencies to report domestic Federal financial assistance award information with particular data elements and to make that information available to Congress, States, and the public. *See* 31 U.S.C. § 6101 *et seq*. The United States Bureau of the Census (Census) serves as the executive agent for the FAADS. One of the required data elements for reporting to FAADS is the Federal Award Identifier Number (FAIN). Originally, Census released Federal assistance award information reported to the FAADS in the form of a CD-ROM. In 1996, Census began making the data available through an internet website as well as through continued CD-ROM distribution.

Officials in the Office of the Chief Financial Officer immediately recognized the potential sensitivities of what had been learned on Friday, April 13 and that same day had the identification numbers associated with the USDA funding removed from the Federal FAADS website so that they could further investigate the situation. In addition, at the request of the Office of Management and Budget (OMB), OMB Watch removed all FAIN numbers for all entities on its FedSpending.org website. The Office of the Chief Information Officer obtained a list of entities that received the CDs from Census, and has been actively contacting these entities to request destruction of the CDs. Here is what they learned by the first of last week:

Many years ago the predecessor agencies to the Farm Service Agency (FSA) and Rural Development (RD) established identification numbers for borrower or grantee applicants and loan files. For some, but not all programs, they adopted as the unique file identifier a number that consisted of a combination of the SSN of the recipient or borrower and other agency assigned values. In some cases, it is possible that individual borrowers or recipients functioning in an entrepreneurial capacity used a SSN instead of an Internal Revenue Service (IRS) issued EIN. Federal law has long required that Federal agencies collect the SSN or EIN of entities and individuals receiving financial awards from the Federal government to report income to the IRS or perform debt collection activities.

When the predecessor agencies to the Farm Service Agency (FSA) and Rural Development (RD) began providing USDA grant and loan award data to FAADS as required in 1982, they simply used the Agency created code as the Federal Award Identification Number (FAIN) for FAADS. Pursuant to the direction from OCIO last summer, USDA agencies searched for the presence of SSNs in their systems, but the FAINs eluded attention because the sensitive information was not readily apparent when viewing the aggregated data.

During the week of April 16th the week immediately following the discovery on Friday, April 13, USDA first analyzed the potential breadth of the problem. After evaluation of approximately 3 million detailed original award and award modification records spanning a period of 26 years, it was determined that the information provided by the Farm Service Agency (FSA) and Rural Development (RD) to the public website in question contained sensitive information relating to approximately 38,700 persons.

Approximately 35,000 of the individuals participated in one of the following FSA programs:

- Seed Loans;
- Emergency Loans;
- Farm Ownership Loans;
- Apple Loans; and
- Soil and Water Loans and Horse Breeder Loans.

Approximately 3,700 of the affected individuals participated in one of the following RD programs:

- Business and Industry Loans;
- Community Facilities Loans and Grants;
- Single Family Housing Guaranteed Loans Natural Disaster;
- Rural Rental Assistance Payments;
- Rural Rental Housing Loans;
- Rural Rental Housing Guaranteed Loans;
- Farm Labor Housing Loans and Grants; and
- Renewable Energy Systems and Energy Efficiency Improvements Program.

Our team was very deliberate in designing reconciliation between FAADS and our internal USDA files to make sure we considered all recipients, whose records were sent to the system, going back to the inception of the system in 1981.

The initial universe of potential transactions summarized by Recipient Name, Recipient Type, Federal Award Identification Number, State, Catalog of Federal Domestic Assistance Number, and other fields (including each award and subsequent modification for non aggregated transactions) exceeded 700,000 records. Using a combination of the Recipient Type and Recipient Name fields, the USDA team was able to eliminate all transactions that were not made to small businesses or individuals and that contained nine or more numeric digits. This narrowed the potential universe to approximately 189,000 recipients.

USDA's agencies then matched the record sets against their program systems and eliminated an additional number of records as not containing SSNs. Through this methodology, we determined that approximately 38,700 unique SSNs were posted publicly. The design and execution of this methodology took approximately 9 days to complete. Upon completion USDA began mailing letters to the affected individuals on April 23, 2007. We expect all expect that all affected individuals received notification by May 1, 2007.

<u>USDA's Response</u>

USDA's response to this incident is twofold. First, we took immediate steps to protect the individuals whose sensitive information has been exposed. Second, we are stepping up our system wide efforts to protect sensitive data and to further reduce the possibility of a similar incident.

Our immediate first steps were to confine and fix the problem, while at the same time making sure not to take any actions that would make the problem worse. To date, there is no evidence that this information has been misused. USDA is offering 12 months of credit monitoring services to help affected persons monitor their personal accounts. This includes:

- Availability of live customer service agents 24 hours, 7 days a week;
- Subscription for credit monitoring by phone, U.S. Mail, fax, or internet;
- Daily alerts and unlimited reports via internet, or quarterly reports by U.S. Mail;
- Assistance if individuals identity is stolen or misused;

- $20,000 insurance policy for identity theft (Except for the State of New York, where companies are currently unwilling to underwrite identity theft insurance coverage until New York State Legislators pass a bill affirming the legality of identity theft insurance coverage.)

USDA funding recipients whose sensitive information was exposed are being notified via mail and are being provided with instructions on how to register for credit monitoring. In addition, we established a toll free line for recipients with questions to call. They can also visit USA.gov, which has a question and answer page on this incident.

As a result of the recent incident, we have initiated the following additional actions consistent with the recommendations included in the recently submitted report to the President by the Identity Theft Task Force, titled "Combating Identity Theft: A Strategic Plan":

1) We have directed all agencies to re-inventory all the data they collect, either electronically or via paper, to ensure that we have full knowledge at the agency and Department-level of any documents, files, or databases that contain sensitive information;

2) We have directed that all USDA agencies identify to us all Federal and non-Federal entities to which they provide data, the source of that data, whether any sensitive information is included, and the justification for its inclusion. The provision of data to external entities was not assessed in our 2006 inventory data gathering effort;

3) We are undertaking a review of our current Privacy Act training program and will assess its adequacy in communicating the stewardship role USDA has over personal

information, whether or not the data is covered by the Privacy Act, and make the changes required;

4) We have added the safeguarding of sensitive information as control items to be routinely evaluated as part of our Departmental level annual internal control assessment. These controls have historically been assessed at the agency level. Our implementation of a standard Departmental approach to assessing controls over financial reporting has shown that a Departmental adoption of a standard methodology for documenting controls, defining test criteria, and evaluating test results moves us to a scientific measurement of effectiveness thus improving our ability to rely upon these controls.

We believe these actions will get to the root cause of this recent data incident and prevent further occurrences. We will do what is needed to track the results of these efforts and provide the leadership needed to ensure that we provide appropriate protections for sensitive data.

While this incident focuses our attention on protecting sensitive data, USDA is also redoubling its efforts in the area of overall IT Security to emphasize how seriously we take our role as data stewards.

Overall IT Security Initiatives

Of course protection of individuals' sensitive information is just one component of an agency's overall IT security program. USDA has had an ongoing challenge related to IT Security. Annually we review and identify material weaknesses in our internal controls over information technology. A material weakness is a condition in which internal controls do not reduce the risk that significant errors or fraud may occur or not be detected in a timely manner. These weaknesses which were detailed in our Performance and Accountability Report, previously sent to the Congress, include:

1) Access controls, logical – Insufficient controls over access to systems and databases, e.g., weak password parameters;
2) Access controls, physical – Insufficient controls over physical access to locations where systems are housed, e.g., mission critical systems operated outside of controlled data centers;
3) Software Change Controls – Insufficient controls over changes made to software, e.g., changes made to software without testing;
4) Disaster Recovery – Lack of timely recovery capabilities for mission critical systems.

These material weaknesses were previously identified, and although progress has been made, they remain on the list. To bring additional senior oversight to the resolution of the information technology problems, we assigned the Deputy Chief Financial Officer and the Deputy Chief Information Officer to coordinate and oversee all USDA agencies efforts to remedy these IT weaknesses. In areas where full remediation of a weakness will take an extended period of time, e.g., when only a full system replacement will completely fix the underlying weakness, they are ensuring that the USDA agencies implement immediate short-term solutions to ensure that our IT resources and data cannot be compromised.

In closing, I want to again state we regret the incident occurred and are committed to taking care of the individuals affected and to fix the problems which led to this issue. We would be pleased to report back to the Committee on our progress and IT issues. We know it is important and the responsibility of everyone to protect the information of individuals with whom the Department does business.

Mr. Chairman, we would be pleased to respond to any questions from the Committee.